

What is claim d is:

1 1. A method for protecting data generated by a
2 keyboard, comprising the steps of:
3 reading data from a keypad of the keyboard;
4 encrypting the read data; and
5 transmitting the encrypted data from the keyboard
6 to a computer.

1 2. The method of claim 1 further comprises the
2 steps of receiving the transmitted encrypted data by the
3 computer; and
4 decrypting the received encrypted data by the
5 computer.

1 3. The method of claim 1 wherein the step of
2 transmitting comprises the step of using a wireless link over
3 which the encrypted data is transmitted.

1 4. The method of claim 1 wherein the step of
2 encrypting comprises the step of using an encryption seed;
3 and
4 entering the encryption seed via the keypad.

1 5. The method of claim 1 wherein the step of
2 encrypting comprises the step of using an encryption seed;
3 and
4 receiving the encryption seed from at least one of
5 the computer or a server.

1 6. The method of claim 1 wherein the step of

2 encrypting comprises the step of using an encryption seed;
3 and
4 reading the encryption seed from a device reader
5 connected to the keyboard.

1 7. The method of claim 6 wherein the step of
2 reading the encryption seed comprises the step of enabling
3 the device reader with a personal identification number.

1 8. The method of claim 1 wherein the step of
2 encrypting comprises the step of receiving a start signal.

1 9. The method of claim 8 wherein the step of
2 receiving the start signal comprises the step of generating
3 the start signal by at least one of a special key on keyboard,
4 multi-actuation of a number of keys on the keypad, the
5 computer, or a server.

1 10. The method of claim 1 wherein the step of
2 encrypting comprises the step of receiving a stop signal that
3 stops the encryption.

1 11. The method of claim 10 wherein the step of
2 receiving the stop signal comprises the step of generating
3 the stop signal by at least one of a special key on keyboard,
4 multi-actuation of a number of keys on the keypad, the
5 computer, or a server.

1 12. The method of claim 1 further comprises the
2 step of defining operations of the step of encrypting from
3 program information received from at least one of a device

4 reader, the computer, or a server.

1 13. A method for protecting by a computer data
2 generated by a keyboard where the keyboard is connected
3 to the computer, comprising the steps of:

4 receiving encrypted data from the keyboard by the
5 computer; and

6 decrypting the encrypted data.

1 14. The method of claim 13 wherein the step of
2 decrypting comprises the step of performing operations of
3 decryption by at least one of a keyboard driver executing on
4 the computer or an application executing on the computer.

1 15. The method of claim 13 wherein the step of
2 decrypting comprises the step of using a seed.

1 16. The method of claim 15 wherein the step of
2 using comprises the step of reading the encryption seed from
3 a device reader connected to the computer.

1 17. The method of claim 16 wherein the step of
2 reading the encryption seed comprises the step of enabling
3 the device reader with a personal identification number.

1 18. The method of claim 13 further comprises the
2 step of generating a start signal to cause the keyboard to
3 start encrypting data.

1 19. The method of claim 13 further comprises the
2 step of generating a stop signal to cause the keyboard to

3 stop encrypting data.

1 20. The method of claim 13 further comprises the
2 step of transmitting program information to the keyboard to
3 define encryption operations.

1 21. A method for protecting by a server data
2 generated by a keyboard where the keyboard is connected
3 to the server via a network and a computer, comprising the
4 steps of:

5 receiving encrypted data from the keyboard by the
6 server; and
7 decrypting the encrypted data.

1 22. The method of claim 21 wherein the step of
2 decrypting comprises the step of performing operations of
3 decryption an application executing on the server.

1 23. The method of claim 21 further comprises the
2 step of generating a start signal to cause the keyboard to
3 start encrypting data.

1 24. The method of claim 21 further comprises the
2 step of generating a stop signal to cause the keyboard to
3 stop encrypting data.

1 25. The method of claim 21 further comprises the
2 step of transmitting program information to the keyboard to
3 define encryption operations.

1 26. A keyboard for encrypting data before

2 transmission to a computer connected to the keyboard via a
3 link, comprising:
4 an interface connected to the link;
5 a memory;
6 a keypad for generating the data;
7 a processor for encrypting the generated data by
8 execution of an encryption routine stored in the memory; and
9 transmitting the encrypted data to the computer via
10 the interface and link.

1 27. The keyboard of claim 26 wherein the link is a
2 wireless link.

1 28. The keyboard of claim 26 comprises a device
2 reader for reading a device to obtain a seed for the
3 encryption routine.

1 29. The keyboard of claim 26 comprises the
2 processor executing a control routine to receive the
3 encryption routine from at least one of the computer or a
4 server and to store the received encryption routine in the
5 memory.

1 30. The keyboard of claim 26 comprises a special
2 key which when actuated causes the processor to at least
3 start executing the encryption routine or stop executing the
4 encryption routine.

1 31. A processor-readable medium for protecting
2 data generated by a keyboard, comprising processor-

3 executable instructions configured for:
4 reading data from a keypad of the keyboard;
5 encrypting the read data; and
6 transmitting the encrypted data from the keyboard
7 to a computer.

1 32. The processor-readable medium of claim 31
2 wherein the transmitting comprises using a wireless link over
3 which the encrypted data is transmitted.

1 33. The processor-readable medium of claim 31
2 wherein the encrypting comprises using an encryption seed;
3 and
4 entering the encryption seed via the keypad.

1 34. The processor-readable medium of claim 31
2 wherein the encrypting comprises using an encryption seed;
3 and
4 receiving the encryption seed from at least one of
5 the computer or a server.

1 35. The processor-readable medium of claim 31
2 wherein the encrypting comprises using an encryption seed;
3 and
4 reading the encryption seed from a device reader
5 connected to the keyboard.

1 36. The processor-readable medium of claim 35
2 wherein the reading the encryption seed comprises enabling
3 the device reader with a personal identification number.

1 37. The processor-readable medium of claim 31
2 wherein the encrypting comprises receiving a start signal.

1 38. The processor-readable medium of claim 37
2 wherein the start signal is generated by at least one of a
3 special key on keyboard, multi-actuation of a number of keys
4 on the keypad, the computer, or a server.

1 39. The processor-readable medium of claim 31
2 wherein the encrypting comprises receiving a stop signal that
3 stops the encryption.

1 40. The processor-readable medium of claim 39
2 wherein the stop signal generated by at least one of a
3 special key on keyboard, multi-actuation of a number of keys
4 on the keypad, the computer, or a server.

1 41. The processor-readable medium of claim 31
2 further comprises receiving processor-executable
3 instructions for the encrypting from at least one of a device
4 reader, the computer, or a server.

1 42. An apparatus for executing the steps of
2 claim 1.

1 43. An apparatus for executing the steps of
2 claim 2.

1 44. An apparatus for executing the steps of
2 claim 4.

1 45. An apparatus for executing the steps of
2 claim 5.

1 46. An apparatus for executing the steps of
2 claim 6.

1 47. An apparatus for executing the steps of
2 claim 9.

1 48. An apparatus for executing the steps of
2 claim 12.